REMARKS/ARGUMENTS

In the Office Action mailed April 16, 2009, claims 1-9 were rejected. Claims 1-10 were objected to for various reasons. Additionally, the specification was objected to. In response, Applicant hereby requests reconsideration of the application in view of the amendments and the below-provided remarks.

For reference, claims 1-10 are amended. In particular, these claims are amended to clarify the language of the claims. Claim 8 is also amended to recite similar limitations in independent form, without depending from the method of claim 1. Claim 10 is also amended to remove the multiple claim dependency. These amendments are supported, for example, by the original language of the claims.

Also, claims 11-13 are added. Claims 11 and 12 are added to recite limitations related to subject matter previously recited in claim 1. Claim 13 is added to recite limitations related to subject matter previously recited in claim 2. These new claims are supported, for example, by the original language of claims 1 and 2.

Objections to the Specification

The Office Action suggests that section headings be added to the specification, according to the guidelines set forth in the MPEP. Applicant notes that the suggested section headings are not required and, hence, Applicant respectfully declines to amend the specification to include the indicated section headings.

Objections to the Claims

The Office Action objects to claims 1-10 for several reasons. In particular, claims 1-10 are objected to because the claims do not recite active words that would be appropriate to set forth steps taken in a method claim. Also, claims 1, 2, and 7 are objected to because the claim language causes ambiguities which make examination difficult. Also, claim 10 is object to as being in improper form for a multiple dependent claim.

In regard to the use of active words, Applicant submits that claims 1-7 and 10 are amended to recite active words appropriate to set for the operations of the method.

Accordingly, Applicant respectfully requests that the indicated objections of claims 1-7 and 10 be withdrawn. Also, claims 8 and 9 are amended to separately recite an apparatus in independent form. Hence, the indicated objections are not applicable to the amended language of claims 8 and 9.

In regard to the ambiguities, Applicant submits that the claims are amended to clarify the language of the claims. In particular, instances of "and/or" are removed, and in some cases new claims are added to separately recite limitations previously recited together in a single claim.

In regard to the form of claim 10, Applicant submits that claim 10 is amended to remove the multiple claim dependency. Hence, there is no question of whether or not the use of multiple claim dependency might be proper.

In light of the amendments to the claims. Applicant respectfully submits that the indicated objections are overcome or no longer apply. Accordingly, Applicant requests that the objections to the claims be withdrawn.

Claim Rejections under 35 U.S.C. 112

Claims 1, 2, and 7-10 were rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention. In particular, claim 1 was rejected because the claims are generally narrative. Also, claims 1, 2, 7, 9, and 10 were rejected for including the term "and/or" which renders the scope of the claims unascertainable. Also, claims 7-9 were rejected as being incomplete for omitting essential structural cooperative relationships of elements because the claims do not provide any functional interrelationship to any software and hardware structural components to provide the operations of the method of claim 1.

In regard to the use of narrative language, Applicant submits that the claims are amended to more clearly set for the limitations of each claim. In particular, the claims are amended to correct grammatical and idiomatic errors.

In regard to the use of "and/or" in the claims, Applicant submits that the claims are amended to delete the indicated language from the claims. Thus, the term "and/or" is not used in the claims.

In regard to the structural cooperative relationships, Applicant submits that claim 7 is amended to more clearly relate to and depend from the method of claim 1. Also, claims 8 and 9 are amended to independently recite an apparatus in the form of a microprocessor and a smart card, respectively.

In light of the amendments to the claims. Applicant respectfully submits that the indicated rejections are overcome or no longer apply. Accordingly, Applicant requests that the indicated rejections under 35 U.S.C. 112, second paragraph, be withdrawn.

Claim Rejections under 35 U.S.C. 101

Claims 1-6 were rejected under 35 U.S.C. 101 as being directed to non-statutory subject matter. In particular, the Office Action states that claims 1-6 do not qualify as a statutory process because the claims are not tied to a particular machine and do not transform underlying subject matter.

Applicant submits that claims 1-6 qualify as a statutory process because the method recited in the claims is tied to a particular machine. Specifically, claim 1 refers to a "hyperelliptical public key cryptosystem." Within the context of the present application, the cryptosystem is implemented, for example, within hardware such as a microprocessor and/or a chip card and/or a smart card. Thus, the reference in claim 1 to a hyperelliptic public key cryptosystem ties the claimed process to a particular machine. Moreover, the claimed method is not merely a mental process because an implementation of the hyperelliptic public key cryptosystem could not occur in the absence of a specific machine. Additionally, the claimed method is not merely a mental process because a differential power analysis attack could not occur in the absence of a specific machine (i.e., the hyperelliptic public key cryptosystem).

Therefore, the reference to the hyperelliptic public key cryptosystem is a reference to a particular machine to which the claimed method is tied, and the method of claims 1-6 is a statutory process because the method is tied to the hyperelliptic public key cryptosystem. Accordingly, Applicant respectfully requests that the rejections under 35 U.S.C. 101 be withdrawn.

Claim Rejections under 35 U.S.C. 102 and 103

Claims 1-4 were rejected under 35 U.S.C. 102(b) as being anticipated by Coron et al. ("Resistance Against Differential Power Analysis for Elliptic Curve Cryptosystems" 1999, pages 1-11, hereinafter Coron). Additionally, claims 5 and 6 were rejected under 35 U.S.C. 103(a) as being unpatentable over Coron in view of Lange ("Weighted Coordinates on Genus 2 Hyperelliptic Curves" October 11, 2002, pages 1-20, hereinafter Lange). Additionally, claims 7-9 were rejected under 35 U.S.C. 103(a) as being unpatentable over Coron in view of Okeya et al. (U.S. Pat. Pub. No. 2003/0059-42, hereinafter Okeya). Additionally, claim 1 was rejected under 35 U.S.C. 102(b) as being anticipated by Joye et al. ("Protections against Differential Analysis for Elliptic Curve Cryptography" Springer-Verlag, 2001, pages 1-15, hereinafter Joye). However, Applicant respectfully submits that these claims are patentable over Coron, Lange, Okeya, and Joye for the reasons provided below.

Independent Claim 1

Claim 1 is patentable over both Coron and Joye (used in separate 102 rejections) because the cited references do not disclose all of the limitations of the claim. Claim 1 recites:

> A method for defence against an attack made by means of differential power analysis, the method comprising:
>
> randomizing at least one factor in at least one hyperelliptic public key cryptosystem, which is given by at least one hyperelliptic curve of any genus over a finite field in a first group, where the hyperelliptic curve is given by at least one coefficient, wherein the factor is selected from the group consisting of:
>
> the hyperelliptic curve; and
>
> at least one element of the first group.

(Emphasis added.)

In contrast, neither Coron nor Joye discloses a hyperelliptic public key cryptosystem and use of a hyperelliptic curve. For reference, hyperelliptic curve cryptosystems use a hyperelliptic curve, which is based on the following equation (or a similar equation):

$$y^2 + h(x)y = f(x)$$

In contrast to a hyperelliptic curve cryptosystem, Coron and Joye are directed instead to elliptic curve cryptosystems. Coron is specifically directed to an elliptic curve cryptosystem for differential power analysis attacks. Coron, abstract. Similarly, Joye is specifically directed to methods to protect scalar multiplication on an elliptic curve against differential analysis. Joye, abstract. In general, elliptic curve cryptosystems use an elliptic curve which is based on the following equation (or a similar equation):

$$y^2 + xy = x^3 + ax^2 + b$$

Thus, elliptic curve cryptosystems are different from hyperelliptic curve cryptosystems, at least because each type of cryptosystem uses a distinct curve equation. Therefore, Coron and Joye do not disclose a hyperelliptic public key cryptosystem and use of a hyperelliptic curve because Coron and Joye merely describe elliptic curve cryptosystems and using an elliptic curve.

For the reasons presented above, Coron and Joy do not disclose all of the limitations of the claim because both Coron and Joye fail to disclose a hyperelliptic public key cryptosystem and use of a hyperelliptic curve, as recited in the claim. Accordingly, Applicant respectfully asserts claim 1 is patentable over each of Coron and Joye because Coron and Joye fail to disclose all of the limitations of the claim.

Independent Claim 8

Applicant respectfully asserts independent claim 8 is patentable over the cited references at least for similar reasons to those stated above in regard to the rejections of independent claim 1. Claim 8 recites subject matter which is similar to the subject matter of claim 1 discussed above. Although the language of this claim differs from the language of claim 1, and the scope of this claim should be interpreted independently of other claims, Applicant respectfully asserts that the remarks provided above in regard to the rejection of claim 1 also apply to the rejection of claim 8.

Dependent Claims

Claims 2-7 and 9-13 depend from and incorporate all of the limitations of the corresponding independent claims 1 and 8. Applicant respectfully asserts claims 2-7 and 9-13 are allowable based on allowable base claims. Additionally, each of claims 2-7 and 9-13 may be allowable for further reasons.

CONCLUSION

Applicant respectfully requests reconsideration of the claims in view of the amendments and the remarks made herein. A notice of allowance is earnestly solicited.

At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account **50-4019** pursuant to 37 C.F.R. 1.25. Additionally, please charge any fees to Deposit Account **50-4019** under 37 C.F.R. 1.16, 1.17, 1.19, 1.20 and 1.21.

Respectfully submitted,

/mark a. wilson/

Date: July 16, 2009

Mark A. Wilson
Reg. No. 43,994

Wilson & Ham
PMB: 348
2530 Berryessa Road
San Jose, CA 95132
Phone: (925) 249-1300
Fax: (925) 249-0111